

CLAIMS

What is claimed is:

1. A system that facilitates access to a plurality of shared software objects by disparate entities, comprising:
 - a platform component that receives a request to access an object by an entity;
 - a data store that stores security information on classes of the objects; and
 - a verification component that employs the security information to verify that the entity has permission to call an API for the object and/or operate on the object.
2. The system of claim 1, the verification component exposes the object if permission exists.
3. The system of claim 1, the verification component masks the object if permission does not exist.
4. The system of claim 1, the platform further comprising a Subscription Platform Service to facilitate automated billing and provisioning of accounts.
5. The system of claim 1, the verification component facilitates that partners receive full access to Application Programming Interfaces (API's) and/or objects for which there is a business need and partial or limited access to other API's or business objects.
6. The system of claim 1, the data store provides default or determined security information related to a class.
7. The system of claim 6, further comprising a component to override the default security information with higher or different security options.

8. The system of claim 1, further comprising a component that supports proxied tenant callers wherein an intermediate proxy places calls into a subscription platform service on behalf of another tenant and achieves access to selected objects.
9. The system of claim 1, further comprising a management portal to facilitate authorization of information.
10. The system of claim 1, further comprising a component to provide an explicit security mapping for an object.
11. The system of claim 1, further comprising a component to enable an implicit security mapping from an explicitly mapped object or to derive an implied security permission by utilizing related objects.
12. The system of claim 1, the verification component employs operating system identities to facilitate security authorization procedures.
13. The system of claim 1, further comprising at least one of a sign-up API caller, an account management API caller, and a customer care API caller.
14. The system of claim 13, further comprising at least one API related to at least one of a sign-up API group, an account management API group, a customer care API group, and an object designer API group.
15. The system of claim 1, further comprising authorization logic that determines whether an API can access an object *via* an access rights set.
16. The system of claim 1, further comprising at least one of a restricted audience offer, a conversion component, and a payment instrument component.

17. A computer-readable medium having computer-executable instructions stored thereon to perform at least one of the platform component and the verification component of claim 1.
18. A method to facilitate security for subscription objects, comprising:
 - storing one or more security options in a database, the security options related to an automated billing and provisioning system;
 - assigning the security options to a class; and
 - inheriting the security options by object members of the class.
19. The method of claim 18, further comprising at least one of explicitly and implicitly assigning the security options to the object members of the class.
20. The method of claim 18, further comprising accessing the database *via* an application programming interface (API).
21. The method of claim 20, further comprising automatically authorizing the API.
22. The method of claim 21, further comprising returning an error code if an authorization procedure fails.
23. The method of claim 21, further comprising analyzing a simple object access protocol request.
24. The method of claim 21, further comprising analyzing one or more security credentials.
25. The method of claim 24, further comprising employing a cache to process the credentials.

26. The method of claim 18, the automated billing and provisioning system further comprising a Subscription Platform Service.
27. The method of claim 18, the security options are associated with default security parameters.
28. The method of claim 18, further comprising overriding the default security parameters with other security options.
29. The method of claim 18, further comprising employing an intermediate proxy that places calls into a subscription platform service on behalf of another tenant.
30. A system to facilitate business object security, comprising:
 - means for authenticating at least one entity attempting access to an online billing and service;
 - means for authorizing the at least one entity; and
 - means for associating a security parameter with at least one business object from a globalized region of a database.
31. A signal to facilitate communications between at least two components of an subscription platform service, comprising:
 - a data packet comprising:
 - an Application Programming Interface packet to identify a partner;
 - a security credential packet to facilitate authorization of the partner; and
 - a security parameter packet inherited by a business object to facilitate access to a subscription platform database.

32. A computer readable medium having a data structure stored thereon, the data structure comprising:

at least one security field indicating global security parameters in a subscription platform database;

at least one object field associated with an account in the database; and

at least one class field to associate the security field and the object field.